ATTENTI ALLE TRUFFE

CONSIGLI PER LA PREVENZIONE DELLE TRUFFE ALLE PERSONE ANZIANE

TRUFFE DOMESTICHE

TRUFFA DEI FINTI APPARTENENTI ALLE FORZE DELL'ORDINE

Una telefonata di un finto appartenente alle Forze dell'Ordine o di un finto avvocato fa credere alla vittima che un proprio parente sia rimasto coinvolto in un incidente stradale o che sia stato arrestato. Alla vittima verrà richiesta una somma di denaro a titolo di corrispettivo per fornire assistenza sanitaria o legale alla persona cara in difficoltà. Se la persona truffata accetta, l'interlocutore comunica che di lì a breve un assistente o un Carabiniere in borghese si recherà presso l'abitazione per ritirare il denaro contante.

CONSIGLI:

- *Diffida delle apparenze*
- *Non aprire mai la porta agli sconosciuti*
- *Non fidarti del solo tesserino di riconoscimento: non basta!*
- *Ricorda che le Forze dell'Ordine non chiedono mai denaro per assistere i cittadini*

TRUFFA DEL FINTO NIPOTE

I truffatori chiamano la vittima al telefono, iniziando la conversazione con frasi trabocchetto come “Indovina un po’ chi parla!” o “Zia/o, ti ricordi di me?”. In questo modo cercano di cogliere il nome di un parente o di un conoscente. Fingendo di essere questa persona, raccontano di aver urgente bisogno di denaro per gravi motivi, ma che non sono in grado di passare a ritirare i soldi. Se la vittima accetta, l’interlocutore comunica che di lì a breve un amico si recherà presso l’abitazione a ritirare la somma o invita la vittima a fare un bonifico sul proprio conto.

CONSIGLI:

- *Diffida delle apparenze*
- *Non aprire mai la porta agli sconosciuti*
- *Non fidarti del solo tesserino di riconoscimento: non basta!*
- *Limitate la confidenza al telefono: in caso di persone che si presentano come parenti e vi chiedono denaro, prendete tempo e chiamate il numero unico di emergenza 112 o un parente*

TRUFFA DEI FINTI RAPPRESENTANTI COMPAGNIE DI FORNITURA

Il truffatore si presenta a casa della vittima spacciandosi per rappresentante di una compagnia fornitrice di servizi (acqua, luce o gas), informando la vittima di nuove e più vantaggiose condizioni contrattuali. Con questo stratagemma, il malintenzionato ottiene la fiducia della vittima per raccoglierne i dati, successivamente utilizzati per aprire nuovi contratti a suo nome ma senza il suo consenso.

CONSIGLI:

- *Diffida delle apparenze*
- *Non aprire mai la porta agli sconosciuti*
- *Non fidarti del solo tesserino di riconoscimento: non basta!*
- *Contatta la compagnia di fornitura ai numeri di telefono presenti sulle bollette (non chiamare utenze telefoniche fornite dallo sconosciuto alla porta)*
- *Non firmare nulla e chiedi sempre consiglio a persone di fiducia più esperte*

FINTI TECNICI COMPAGNIE DI FORNITURA
(TRUFFA DEL CONGELATORE)

I truffatori, travestiti da tecnici dell'acqua o del gas, si presentano alla porta della vittima riferendo che in casa c'è un grave problema da risolvere immediatamente. Sfruttando l'ansia e la preoccupazione della vittima, i truffatori la invitano a proteggere i propri beni preziosi da potenziali fughe di gas o altre minacce, mettendoli al sicuro in un sacchetto all'interno del congelatore, che poi abilmente sottraggono.

CONSIGLI:

- *Diffida delle apparenze*
- *Non aprire mai la porta agli sconosciuti*
- *Non fidarti del solo tesserino di riconoscimento: non basta!*
- *Contatta la compagnia di fornitura*
- *Se hai fatto entrare sconosciuti in casa, non farti distrarre e, senza perdere la calma, invitali con decisione ad uscire*
- *Ricorda che nessun ente o società manda i propri dipendenti in visita a domicilio per riscuotere pagamenti*
- *Tutte le aziende di servizi (gas, luce, acqua e telefono) annunciano sempre il loro arrivo con avvisi al condominio, comunicati molto tempo prima*

TRUFFA DEL CALL CENTER

Il truffatore contatta telefonicamente la vittima, spacciandosi per un call center. Il finto operatore fa domande banali per indurre la vittima a rispondere con un “sì”, che verrà poi estrapolato e utilizzato come forma di assenso per l’attivazione di un nuovo contratto di fornitura. La vittima si accorge della truffa al momento della ricezione della prima bolletta.

CONSIGLI:

- Diffida delle apparenze

- Se non si comprende l’identità della persona chiamante, dovete fare domande ed evitare di rispondere fornendo i propri dati personali

- In caso di contratto o attivazione non richiesti, inviare un reclamo scritto al fornitore con raccomandata A/R o pec

- Limitate la confidenza al telefono: in caso di persone che si presentano come parenti e vi chiedono denaro, prendete tempo e chiamate il parente che sostiene di avervi contattato, per verificare che lo abbia effettivamente fatto o il numero unico di emergenza 112

TRUFFA DELLA FALSIFICAZIONE DELL'IDENTITA'
(CD. "SPOOFING")

Il truffatore contatta la vittima attraverso un finto call center utilizzando, grazie ad appositi programmi informatici, numeri di telefono corrispondenti ai numeri verdi degli istituti bancari. Carpita la fiducia della vittima e ottenute le credenziali di accesso al conto corrente, procede a spostare il denaro su appositi conti dotati di carte virtuali

CONSIGLI:

- *Non condividere telefonicamente i dati personali né quelli di accesso al conto corrente*
- *Limitate la confidenza al telefono: in caso di persone che vi chiedono denaro, prendete tempo e chiamate il numero unico di emergenza 112*

TRUFFE FUORI CASA

TRUFFA DEL FALSO AMICO

Il truffatore si avvicina alla vittima, abbracciandolo improvvisamente e fingendo di conoscerlo. Di solito si presenta come un amico dei figli o dei nipoti e coinvolge la persona truffata in una lunga conversazione per distrarlo e fargli credere di riconoscerlo. Gli racconta di aver accumulato un debito nei confronti della banca o di persone poco raccomandabili e convince la vittima a dargli denaro contante o gioielli.

CONSIGLI:

- *Quando si esce, non portare con sé grosse somme di denaro*
- *Quando si paga al bar, non mostrare il denaro o oggetti di valore che si hanno al seguito*
- *Cammina in zone illuminate e frequentate da tante persone*

TRUFFA DELLO SPECCHIETTO

Il truffatore fa credere alla vittima in auto di aver involontariamente la sua autovettura. La vittima sente il rumore di un colpo secco sulla propria carrozzeria, di solito sulla fiancata (provocato in realtà dal truffatore tramite un sasso o un bastone). Il truffatore chiede alla vittima di constatare il danno e di corrispondere una somma di denaro per evitare la denuncia all'assicurazione, ricorrendo, se necessario, a toni aggressivi.

CONSIGLI:

- *Resta in auto senza scendere dal veicolo*
- *Chiudi i finestrini posteriori e lato passeggero per evitare che eventuali complici possano rubare i tuoi oggetti personali*
- *Pretendi da subito di chiamare la Polizia locale o il numero unico di emergenza 112*

TRUFFA DEL BANCOMAT (CD. “SKIMMING”)

Il truffatore altera lo sportello ATM della banca, installando un lettore (detto “skimmer”) o una videocamera e una finta tastiera per clonare le carte di credito e memorizzare i dati digitati.

CONSIGLI:

- *Ispeziona accuratamente lo sportello ATM prima di utilizzarlo, verificando che non ci sia nulla di diverso o anomalo*
- *Copri il tastierino mentre digiti il PIN*

TRUFFA DELLE BANCONOTE BLOCCATE (CD. “CASH TRAPPING”)

Al momento del prelievo allo sportello ATM della banca, alcune banconote restano incastrate nell’erogatore. Non si tratta di un problema tecnico ma di uno stratagemma del truffatore, il quale ha inserito un oggetto metallico nell’erogatore, per poi tornare a recuperare le banconote.

CONSIGLI:

- Resta davanti al bancomat e contatta immediatamente il servizio clienti della banca o il numero unico di emergenza 112

TRUFFE SUL WEB

TRUFFA DELL'EMAIL INGANNEVOLE (CD. "PHISHING")

Il truffatore invia alla vittima un messaggio/e-mail ingannevole, con cui comunica l'avvenuta vincita di una grossa somma di denaro a una lotteria o un qualche tipo di premio. A quel punto, alla vittima viene richiesto di compiere un'azione (esempio, cliccare su un link o scaricare un'App) per carpire i suoi dati personali allo scopo di accedere ai conti bancari o per altre operazioni criminali.

CONSIGLI:

- *Installa un programma antivirus sul tuo p.c. e tienilo aggiornato*
- *Presta attenzione all'indirizzo e-mail completo del mittente e alla presenza di errori ortografici nel testo*
- *Non aprire mai le e-mail ricevute da mittenti sconosciuti*
- *Non cliccare mai sul link presente nelle e-mail sospette e, se per errore dovesse accadere, non autenticarsi sul sito falso, ma chiudere immediatamente il web browser*
- *Non rispondere mai a e-mail in cui ti viene chiesto di dare i tuoi dati personali, con utenza, password, codici di sicurezza e dati relativi alle carte di pagamento*
- *Modifica immediatamente le tue password e attiva l'autenticazione a due fattori, se hai condiviso i tuoi dati*
- *Se hai condiviso i dati di pagamento, contatta subito il tuo istituto bancario per bloccare gli strumenti di pagamento*

TRUFFA DEL FINTO SMS (CD. “SMISCHING”)

Il truffatore invia alla vittima un SMS, al fine di acquisire informazioni personali, finanziarie o di sicurezza chiedendo alla vittima di cliccare su un link e/o di inserire i propri dati personali su un sito web malevolo. In altri casi il truffatore invia un SMS alla vittima da un numero sconosciuto, fingendosi un figlio o un parente e comunicando di avere il cellulare rotto. A quel punto il truffatore chiede l’invio di un messaggio di risposta con dati personali della vittima.

CONSIGLI:

- *Non aprire mai messaggi ricevuti da mittenti sconosciuti*
- *Non rispondere mai a sms in cui ti viene chiesto di dare i tuoi dati personali, con utenza, password, codici di sicurezza e dati relativi alle carte di pagamento*
- *Modifica immediatamente le tue password e attiva l’autenticazione a due fattori se hai condiviso i tuoi dati*
- *Se hai condiviso i dati di pagamento, contatta subito il tuo istituto bancario per bloccare gli strumenti di pagamento*

TRUFFA TELEFONICA (CD. “VISHING”)

Il truffatore, attraverso una telefonata, cerca di convincere la vittima a divulgare informazioni personali, finanziarie o di sicurezza o a trasferirgli del denaro, spacciandosi per rappresentante di un’azienda fornitrice di servizi. Solitamente, questo tipo di truffa segue un SMS o un’e-mail ingannevole.

CONSIGLI:

- *Non aprire mai messaggi ricevuti da mittenti sconosciuti*
- *Non rispondere mai a chiamate, anche di call center, in cui ti viene chiesto di dare i tuoi dati personali, con utenza, password, codici di sicurezza e dati relativi alle carte di pagamento*
- *Modifica immediatamente le tue password e attiva l’autenticazione a due fattori se hai condiviso i dati*
- *Se hai condiviso i dati di pagamento, contatta subito il tuo istituto bancario per bloccare gli strumenti di pagamento*

TRUFFA SENTIMENTALE (CD. “LOVE SCAM”)

Il truffatore, attraverso un finto profilo, aggancia la vittima con una richiesta di amicizia sui social, che si tramuta in una presenza - virtuale - costante e marcatamente premurosa. Il truffatore ottiene la fiducia della vittima giocando su false affinità di interessi, sino a prospettare progetti di una vita futura, evitando sempre di incontrarsi di persona. Successivamente avanza richieste di denaro, lamentando problematiche di natura privata, come la salute dei figli o questioni legali, arrivando a minacciare la vittima di diffondere i contenuti delle conversazioni o i suoi dati personali. Una volta ottenuta la prima somma di denaro, i tuffatori continuano a chiedere e ottenere altri soldi, finché la vittima si rende conto, da sola o aiutato dai parenti, di essere vittima di una truffa.

CONSIGLI:

- *Limita la confidenza sul web - Diffida delle richieste di denaro da parte di sconosciuti*

TRUFFA DELLE COMPRAVENDITE ONLINE

Attraverso finti annunci di vendita di prodotti o servizi a prezzi particolarmente vantaggiosi, il truffatore convince le sue vittime a versare una somma di denaro a titolo di caparra, anche di importo rilevante, per poi dileguarsi nel nulla. In questi casi, alla vittima viene richiesto il versamento di denaro con modalità che non offrono tutele per l'acquirente: una carta postepay, ad esempio, permette al truffatore di avere immediata disponibilità della somma e di prelevarla prima che la vittima possa tentare di revocare il pagamento.

CONSIGLI:

- *Diffida delle offerte all'apparenza molto vantaggiose*
- *Chiedi foto di dettaglio dei prodotti che intendi acquistare (es. un particolare poco visibile), così da verificare che il venditore ne abbia concreta disponibilità*
- *Conserva la ricevuta del pagamento ed eventuali* screenshot *delle conversazioni*
- *Utilizza solo metodi di pagamento tracciabili*

TRUFFA DELLE COMPRAVENDITE ONLINE
CON METODO "ALLA NIGERIANA"

Il truffatore contatta la vittima mostrando un particolare interesse per il suo annuncio. Dopo aver ottenuto la fiducia della vittima, il truffatore spiega che effettuerà il pagamento tramite bonifico bancario dall'estero, aggiungendo che per confermare la transazione è necessario pagare una tassa nazionale, pari a una percentuale sul valore del bonifico. Per convincere la vittima, il truffatore si rende disponibile a rimborsare una somma più alta e manderà via email documenti scannerizzati di un presunto funzionario della banca o del ministero che conferma la necessità di pagare la tassa.

CONSIGLI:

- *Non anticipare mai denaro, quando sei tu che devi riceverlo*
- *Diffida di messaggi che non contengono alcuna richiesta di informazione aggiuntiva sull'oggetto messo in vendita né propongono alcun tipo di trattativa*

IN CASO DI EMERGENZA CHIAMARE IL 112

E’ il miglior sistema per agire in sicurezza ed entrare immediatamente in contatto con le Forze dell’Ordine.